明　細　書

暗号／復号装置及び方法

技術分野

この発明は、高いデータ秘守性を保ちデータの同期外れに対する復元性も高い暗号装置、暗号方法および暗号プログラム、復号装置、復号方法および復号プログラム、ならびに、記録媒体に関する。

背景技術

従来から、ディジタルデータの窃取や改竄などの不正利用を防ぐために、伝送されるディジタルデータに対して暗号化処理を施す暗号化技術が実用化されている。第１図は、ディジタルデータの暗号化を行う一例の構成を概略的に示す。暗号化処理を施す前の元データを平文（プレーンテキスト）と称し、平文に暗号化ブロック２００で暗号化が施されて暗号文（暗号化データ）が生成される。暗号文は、暗号化ブロック２００に対応する復号化ブロック２０１により暗号を復号化され、元の平文に戻される。

暗号化ブロック２００に用いられる暗号化方式としては、例えばＡＥＳ(Advanced Encryption Standard)やＤＥＳ(Data Encryption Standard)が代表的である。ＡＥＳおよびＤＥＳは、何れも秘密鍵と称される公開されない鍵を用いて平文を暗号化および暗号文の復号化を行う。例えば暗号化ブロック２００がＡＥＳにより暗号化を行う場合、暗号化ブロック２００に入力された平文に対して、秘密鍵である鍵２０２を用いて暗号化を施す。暗号化された暗号文は、伝送経路を経由して復号化ブロック２０１に供給され、暗号化の際に用いられたのと

同じ鍵２０２を用いて復号化され、元の平文に戻される。これらＡＥＳやＤＥＳは、暗号化と復号化において共通の鍵を用いる共通鍵方式である。

暗号化ブロック２００および復号化ブロック２０１の構成としては、第２図に一例が示されるような、暗号化回路や復号化回路としてＡＥＳやＤＥＳによる暗号器５０（または復号器）をそのまま用いる構成が考えられる。この第２図の構成は、ＥＣＢモード(Electronic CodeBook mode)と称される。第２図の構成において、暗号器５０は、入力された平文Ｍｉを、鍵（Ｋ）を用いて例えばＡＥＳにより暗号化して暗号文Ｃｉを得る。同一の構成において、暗号文Ｃｉを暗号器５０に入力し鍵（Ｋ）を用いて暗号化すると、暗号文Ｃｉが復号化されて元の平文Ｍｉが得られる。

この第２図の構成では、同一の平文が連続的に入力されると、出力される暗号文も同一の値が続いてしまい、平文と暗号文とに基づく鍵（Ｋ）の解読が容易になってしまう。この問題を解決するために、様々な手法が考えられている。

第３図Ａおよび第３図Ｂは、暗号器の出力を入力にフィードバックさせる構成であって、ＣＢＣモード(Cipher Block Chaining mode)と称する。第３図Ａに示される暗号化回路６０においては、平文Ｍｉが ＥＸＯＲ（排他論理和）回路６１を介して暗号器６２に入力され、鍵（Ｋ）を用いて暗号化される。暗号器６２の出力は、暗号文Ｃｉとして出力されると共に、初期値ＩＶとして遅延回路６３により所定の、例えば１ワード分の遅延を与えられてＥＸＯＲ回路６１に供給され、平文Ｍｉとの排他論理和がとられる。このＥＸＯＲ回路６１の出力が暗号器６２に入力される。

第３図Ｂは、対応する復号化回路６５の構成を示す。復号化の際に

は、暗号文Ｃｉを暗号器６２に入力すると共に、初期値ＩＶ（イニシャライズベクタ）として遅延回路６７で所定の、例えば１ワード分の遅延を与えてＥＸＯＲ６８に供給する。暗号文Ｃｉは、暗号器６２で鍵（Ｋ）を用いて暗号化され、ＥＸＯＲ６８により、所定に遅延された初期値ＩＶとの排他論理和をとられて元の平文Ｍｉに復号化され、出力される。

この第３図Ａおよび第３図Ｂに示す構成によれば、初期値ＩＶを変えることで、同一の鍵（Ｋ）を用いても、同一の平文Ｍｉから異なる暗号文Ｃｉが生成される。初期値ＩＶとして平文Ｍｉを暗号化した暗号文Ｃｉを用いているので、同一の平文Ｍｉが連続的に入力されても暗号器６２で暗号化された暗号文Ｃｉは、同一とはならず、上述のＥＣＢモードに比べて暗号文解析が難しくなる。

第４図Ａおよび第４図Ｂは、発生した暗号文Ｃｉの一部を暗号器の入力としてフィードバックさせる構成であって、ＣＦＢモード(Cipher FeedBack mode)と称する。第４図Ａに示される暗号化回路７０においては、ｊビットデータとして入力された平文ＭｉがＥＸＯＲ回路７１に供給され、暗号器７４の出力のうちｊビットと排他論理和がとられ、暗号文Ｃｉとして出力される。この出力は、ビット数をｊビットからｋビットに変換するξ回路７２を介してＤＲ回路７３に供給される。ＤＲ回路７３は、シフトレジスタを有し、入力されたｋビットのデータを入力順にシフトさせ、例えば１２８ビットのデータＸｉを発生させる。データＸｉは、暗号器７４に供給され、鍵（Ｋ）を用いて暗号化され１２８ビットのデータＹｉとされる。このデータＹｉは、擬似的な乱数列であって、入力される平文Ｍｉとで排他論理和をとることで、暗号文Ｃｉが生成される。

第４図Ｂは、対応する復号化回路７５の構成を示す。ｊビットデー

タとして入力された暗号文Ｃｉは、ξ回路７６でｋビットデータに変換されＤＲ回路７８に供給されると共に、ＥＸＯＲ回路７７に供給される。ＤＲ回路７８は、シフトレジスタを有し、供給されたｋビットのデータから例えば１２８ビットのデータＸｉを生成し、暗号器７９に供給する。データＸｉは、暗号器７９で鍵（Ｋ）を用いて暗号化され１２８ビットのデータＹｉとされる。このデータＹｉは、擬似的な乱数列であって、入力された暗号文Ｃｉとの排他論理和をとることで暗号文Ｃｉが元の平文Ｍｉに復号化される。

このＣＦＢモードは、入力された平文Ｍｉや暗号文Ｃｉをシフトレジスタに入力し、それを暗号器に入力して疑似乱数列を発生させるので、連続的に平文Ｍｉが入力されるストリームデータの暗号化に適している一方、暗号化回路７５から出力された暗号化データに例えば伝送系などでエラーが生ずると、シフトレジスタ（ＤＲ回路）が一巡するまでエラーから回復できないという欠点がある。

第５図Ａおよび第５図Ｂは、暗号器の出力だけをフィードバックして疑似乱数を発生させる構成であって、ＯＦＢモード(Output FeedBack mode)と称する。第５図Ａに示される暗号化回路８０では、暗号器８３自身の出力をシフトレジスタを有するＤＲ回路８２を介して暗号器８３に入力し、それを鍵（Ｋ）を用いて暗号化する。暗号器８３から出力されたデータＹｉは、疑似乱数列であって、このデータＹｉのうちｊビットだけをＥＸＯＲ８１回路に供給し、ｊビットデータとして入力される平文Ｍｉとの排他論理和をとることで、平文Ｍｉが暗号文Ｃｉとされ出力される。

第５図Ｂは、対応する復号化回路８５の構成を示す。このＯＦＢモードでは、復号化回路８５は暗号化回路８０と同一の構成とされる。すなわち、ｊビットの暗号文ＣｉがＥＸＯＲ回路８６に入力される。

一方、暗号器８８自身の出力がシフトレジスタを有するＤＲ回路８７を介して暗号器８８に入力され、鍵（Ｋ）を用いて暗号化される。暗号器８８から出力されたデータＹｉは、疑似乱数列であって、このデータＹｉのうちｊビットだけをＥＸＯＲ８６に供給し、入力された暗号文Ｃｉとの排他論理和をとることで、暗号文Ｃｉが平文Ｍｉに復号化される。

このＯＦＢモードは、暗号化回路８０内および復号化回路８５内でフィードバックが完結しているため、伝送系エラーなどの影響を受けないというメリットがある。

第６図Ａおよび第６図Ｂは、カウンタの出力を順次カウントアップしていき、それを暗号器の入力に与える構成であって、カウンタモード(Counter Mode)と称される。すなわち、カウンタモードでは、カウンタの出力が暗号化されて用いられる。第６図Ａに示される暗号化回路９０では、１２８ビット出力のカウンタ９２が順次カウントアップされたカウント値Ｘｉが暗号器９３に入力され、鍵（Ｋ）を用いて暗号化される。暗号器９３から出力されるデータＹｉは、疑似乱数列であって、このデータＹｉのうちｊビットだけをＥＸＯＲ回路９１に供給し、ｊビットで入力された平文Ｍｉとの排他論理和をとることで、暗号文Ｃｉが生成される。

第６図Ｂは、対応する復号化回路９５の構成を示す。このカウンタモードでは、復号化回路９５は暗号化回路９０と同一の構成とされる。すなわち、カウンタ９７で順次カウントアップされたカウント値Ｘｉが暗号器９８に入力され、鍵（Ｋ）を用いて暗号化される。暗号器９８から出力されるデータＹｉは、疑似乱数列であって、このデータＹｉのうちｊビットだけをＥＸＯＲ回路９６に供給し、ｊビットで入力された暗号文Ｃｉとの排他論理和をとることで、暗号文Ｃｉが平文

Ｍｉに復号化される。

上述のように、ＣＦＢモード、ＯＦＢモードおよびカウンタモードでは、暗号文Ｃｉは、暗号化を行った同一の疑似乱数と暗号文Ｃｉとの排他論理和をとることで、復号化される。非特許文献「Douglas R. Stinson、櫻井幸一、「暗号理論の基礎」、共立出版株式会社、１９９６年」に、上述したような種々の暗号化方式が記載されている。

ところで、近年では、映画館などにおいて、例えば映像サーバに蓄積された映像データを再生し、スクリーンに投影して映画の上映を行うようにした、ディジタルシネマシステムが提案されている。このシステムによれば、例えばネットワークを介して配信された映像データや、大容量光ディスクなどの記録媒体に記録された映像データが映像サーバに供給される。そして、映像サーバからプロジェクタに対して例えば同軸ケーブルを介してこの映像データが伝送され、プロジェクタによりスクリーンに映像データに基づく映像が投影される。

映像データは、例えばＨＤ－ＳＤＩ(High Definition-Serial Data Interface)による伝送フォーマットにより、シリアルディジタルデータとして映像サーバからプロジェクタに伝送される。この映像データは、ベースバンドのビデオデータとして伝送され、その伝送レートは、例えば略１．５Ｇｂｐｓ(Giga bits per second)とされる。

このとき、映像データの窃取を防ぐために、映像サーバから出力される映像データを暗号化し、暗号化された映像データを例えば同軸ケーブルに対して出力してプロジェクタに伝送する。ここで、ＨＤ－ＳＤＩのフォーマットにおいて伝送されるコードに制約が無ければ、上述した各暗号化方式を用い、ＨＤ－ＳＤＩの暗号化／復号化システムが実現できることになる。すなわち、映像サーバ側に暗号化回路を設け、出力される映像データに暗号化を施す。また、プロジェクタ側に

映像サーバの暗号化回路に対応する復号化回路を持たせる。映像サーバで暗号化された映像データは、ＨＤ－ＳＤＩのフォーマットに乗せられて同軸ケーブルを介してプロジェクタに伝送され、プロジェクタの復号化回路で暗号を復号化され、ベースバンドのビデオデータに戻される。

しかしながら、実際には、上述のＨＤ－ＳＤＩには、ワード同期用に禁止コードが定義されている。そこで、本願発明の出願人により、この禁止コードを発生させないで暗号化を行う方式が特願２００２－１３５０３９として既に出願されている。また、当該出願の関連出願として、特願２００２－１３５０７９、特願２００２－１３５０９２、特願２００２－１７３５２３および特願２００２－３４９３７３が既に出願されている。

さらに、近年では、ＨＤ－ＳＤＩにおけるビデオデータの暗号化／復号化に関する標準化が進められており、暗号化方式として、第６図Ａおよび第６図Ｂを用いて説明したカウンタモードを用いることが提案されている。この提案によれば、暗号化単位の１２８ビットのデータを分割して用い、分割されたそれぞれのビットに対して下記の３種類のカウンタを適用するようにしている。

（１）暗号器のクロック毎にカウントアップするクロックカウンタ

（２）映像データのライン毎にカウントアップするラインカウンタ

（３）映像データのフレーム毎にカウントアップするフレームカウンタ

これら３種類のカウンタのうち（１）のクロックカウンタは、ラインが更新される毎にリセットされ、（２）のラインカウンタは、フレームが更新される毎にリセットされ、（３）のフレームカウンタは、映像データによる１つのプログラムの開始時に一度だけリセットされ

る。このように、カウント周期およびリセットタイミングが異なる複数のカウンタを組み合わせて用いることで、例えばデータの伝送系において同期外れ、データ欠落などが生じても、失われるすなわち復号できないデータは、最大で１ライン分のデータで済ませることができる。

また、（１）のクロックカウンタや（２）のラインカウンタによるリセットを行っても、（３）のフレームカウンタの値が更新されていくので、同一の疑似乱数列が繰り返されることが無いという利点もある。

これに対して、第４図Ａおよび第４図Ｂを用いて説明したＣＦＢモードを用いる場合には、若し、プログラム開始後のある時点でリセットをかけ、その後リセットをかけないとしたら、上述した同期外れや、データの欠落などの事故が発生した場合、復帰が非常に困難である。つまり、このＣＦＢモードにおいては、暗号化回路の出力をシフトレジスタにより順次シフトさせていったデータを暗号器で鍵（Ｋ）を用いて暗号化し、この暗号器の出力を用いて平文Ｍｉの暗号化を行っている。そのため、暗号化の際にある時点でエラーが発生すると、シフトレジスタによる影響が無くなるまで復号可能なデータが出力されない。換言すれば、ＣＦＢモードにおいては、出力される暗号文Ｃｉは、過去の全ての暗号文Ｃｉに依存しているため、短時間に復元することができない。

勿論、ＣＦＢモードでも、フレーム毎、ライン毎に暗号器の入力をリセットすることが可能である。しかしながら、ＣＦＢモードでフレーム毎、ライン毎にリセットを行った場合、例えば画面全体が黒一色といった均一な入力データが複数フレームにわたって入力された場合には、暗号器から出力される疑似乱数列は、フレーム毎に同一の並び

となってしまう。このようなケースが発生すると、例えば映像サーバとプロジェクタ間で伝送されるデータを窃取して暗号を解読する際の重大なヒントになってしまい、暗号のセキュリティー上、好ましくない。

ここで、上述のディジタルシネマシステムにおける映像データの窃取方法について考える。第７図は、この映像データ窃取を実現するための一例のシステムを概略的に示す。映像データは、映像サーバ２５０で再生されて暗号化され、暗号データとして同軸ケーブル２５１に送り出される。暗号化方式としては、伝送系のエラーに対する復元性を考慮し、上述したカウンタモードにおいて映像データのライン毎、フレーム毎、プログラムの先頭でそれぞれカウンタをリセットする方式を用いる。プロジェクタ２５４側では、本来であれば、プロジェクタ２５４に接続された同軸ケーブル２５１を介して送られてくるデータを受け取り、暗号を復号化してベースバンドの映像データとし、スクリーン２５５に映出する。

映像データの窃取者は、データ窃取記録／交換装置２５２、ビデオカメラ２５６およびビデオデータ記録装置２５７を用意する。データ窃取記録／交換装置２５２は、映像サーバ２５０およびプロジェクタ２５４の間に挿入する。例えば、第７図に示されるように、サーバ２５０とプロジェクタ２５４とを接続すべき同軸ケーブル２５１をデータ窃取記録／交換装置２５２に接続し、データ窃取記録／交換装置２５２の出力を同軸ケーブル２５３でプロジェクタ２５４に送る。ビデオカメラ２５６は、スクリーン２５５に投影された映像を撮影可能に配置される。ビデオカメラ２５６で撮影された映像は、ビデオデータ記録装置２５７に供給され、光ディスクや磁気テープなどの記録媒体に記録される。

このような構成において、窃取者は、映像サーバ２５０から出力される、映像データが暗号化された暗号化データと、映像データに付随するメタデータとをデータ窃取記録／交換装置２５２で記録する。データ窃取記録／交換装置２５２は、映像サーバ２５０から供給された暗号化データの代わりに、予め用意した所定データを、映像サーバ２５０から暗号化データに付随されて供給されたメタデータと共に出力する。このとき、メタデータには手を加えない。なお、データ窃取記録／交換装置２５２で予め用意される所定データは、例えば黒一色の画面を表示するための固定値である。

データ窃取記録／交換装置２５２から出力された所定データとメタデータは、プロジェクタ２５４に供給される。プロジェクタ２５４では、供給された所定データを復号化する。すなわち、所定データが黒一色を表示する固定データである場合、所定データと復号化回路における疑似乱数とが排他論理和演算される。この所定データと疑似乱数とが排他論理和演算されてなる映像データがスクリーン２５５に投影される。

スクリーン２５５に投影される映像は、このように、例えば固定値である所定データに暗号化回路による疑似乱数を作用させたデータに基づくので、絵としては映像サーバ２５０から出力された元の映像データとは全く異なり、ノイズとしか見えないような映像となる。窃取者は、このスクリーン２５５に投影された上述の所定データによる映像をビデオカメラ２５６で撮影し、ビデオデータ記録装置２５７で記録する。このデータ窃取記録／交換装置２５２で記録された暗号化データと、ビデオデータ記録装置２５７で記録された映像データとに基づき、暗号データ化の元の映像データを復元することができる。

すなわち、プロジェクタ２５４の映写性能と、ビデオカメラ２５６

の撮像性能とが理想的なものであれば、これら暗号化データと映像データの排他論理和をとることで、暗号化データの元の映像データを復元できることになるという問題点があった。

現実的には、理想的な性能を備えたプロジェクタ２５４やビデオカメラ２５６は存在しないので、上述の方法でも、正確に元の映像データを復元することはできない。しかしながら、不完全なデータを用いても、上述の演算を行うことで、高い確率で元の映像データの再現を行うことが可能である。

例えば、映像データの性質として、ある画素とその画素に近接した画素とでは、高い相関性があることが知られている。この近接画像の相関性を利用して、上述のような状況下において、正確に再現できなかった画素の値を求めることができる。その結果、その画素（映像データ）を暗号化した際の疑似乱数を絞り込んでいくことができてしまう。これにより、窃取者により、映像データの暗号化の際の鍵（Ｋ）を解読する大きな手がかりを得られてしまうという問題点があった。

一方、映像サーバ２５０から出力される映像データに対して暗号化を行う暗号化方式としてＣＦＢモードを用いれば、この方式では暗号化された暗号化データをフィードバックして入力データの暗号化を行っているため、同一のデータを入力し続けても出力される疑似乱数列が変化する。そのため、上述のような窃取方法では鍵（Ｋ）の手がかりを得ることが困難である。しかしながら、上述したように、ＣＦＢモードは、伝送系のエラーに対する復元性が弱いという問題点があった。これは、実際に映画館での上映などに用いる際に、深刻な問題となりうる。

発明の開示

したがって、この発明の目的は、より秘守性に優れ、尚かつ、伝送系のエラーに対する復元性も高い暗号化を行うことができる暗号装置、暗号方法および暗号プログラム、復号装置、復号方法および復号プログラム、ならびに、記録媒体を提供することにある。

この発明は、上述した課題を解決するために、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウンタと、保持手段で保持されたデータと１または複数のカウンタによる１または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、演算手段から出力された暗号化データの一部または全部を保持手段に入力する経路と、保持手段および１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする暗号装置である。

また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウントのステップと、保持のステップで保持されたデータと１または複数のカウントのステップによる１または複数のカウント値とを暗号化する暗号化のステップと、暗号化

のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有することを特徴とする暗号方法である。

この発明は、入力されたデータの一部または全部をトリガ信号により保持し、保持されたデータをリセット信号によりリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする1または複数のカウントのステップと、保持のステップで保持されたデータと1または複数のカウントのステップによる1または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび1また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび1また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有する暗号方法をコンピュータ装置に実行させることを特徴とする暗号プログラムである。

この発明は、入力されたデータの一部または全部をトリガ信号によ

り保持し、保持されたデータをリセット信号によりリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウントのステップと、保持のステップで保持されたデータと１または複数のカウントのステップによる１または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有する暗号方法をコンピュータ装置に実行させる暗号プログラムが記録されたことを特徴とするコンピュータ装置に読み取り可能な記録媒体である。

また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウンタと、保持手段で保持されたデータと１または複数のカウンタによる１または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、演算手段から出力された暗号化データの一部または全部を保持手段に入力する経路

と、保持手段および１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有する暗号装置で暗号化された暗号化データを復号する復号装置において、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウンタと、保持手段で保持されたデータと１または複数のカウンタによる１または複数のカウント値とを暗号化する暗号化手段と、暗号化手段の出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算手段と、外部から入力された暗号化データの一部または全部を保持手段に入力する経路と、保持手段および１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持手段および１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有することを特徴とする復号装置である。

また、この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウントのステップと、保持のステップで保持されたデータと１または複数のカウントのステップによる１または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の

規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有する暗号方法で暗号化された暗号化データを復号する復号方法において、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウントのステップと、保持のステップで保持されたデータと１または複数のカウントのステップによる１または複数のカウント値とを暗号化する暗号化手段と、暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、外部から入力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有することを特徴とする復号方法である。

この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたは

カウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウントのステップと、保持のステップで保持されたデータと１または複数のカウントのステップによる１または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有する暗号方法で暗号化された暗号化データを復号する復号方法をコンピュータ装置に実行させる復号プログラムにおいて、復号方法は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウントのステップと、保持のステップで保持されたデータと１または複数のカウントのステップによる１または複数のカウント値とを暗号化する暗号化手段と、暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、外部から入力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび１また複数のカウ

ンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有することを特徴とする復号プログラムである。

この発明は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウントのステップと、保持のステップで保持されたデータと１または複数のカウントのステップによる１または複数のカウント値とを暗号化する暗号化のステップと、暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、演算のステップから出力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有する暗号方法で暗号化された暗号化データを復号する復号方法をコンピュータ装置に実行させる復号プログラムが記録されたコンピュータ装置に読み取り可能な記録媒体において、復号方法は、入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により保持されたデータをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号によりカウント値を所定の値にリセットする１または複数のカウントのステップと、保持のステップで保持されたデータと１または複数のカウントのステップによる１または

複数のカウント値とを暗号化する暗号化手段と、暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して入力データを暗号化し、入力データが暗号化された暗号化データを出力する演算のステップと、外部から入力された暗号化データの一部または全部を保持のステップに入力するステップと、保持のステップおよび１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、保持のステップおよび１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有することを特徴とする記録媒体である。

上述したように、この発明では、最終的な暗号化データの一部または全部がトリガ信号により保持されリセット信号によりリセットされる保持された暗号化データとトリガ信号によりカウント値をカウントアップまたはカウントダウンしリセット信号によりカウント値が所定の値にリセットされる１または複数のカウント値とを暗号化した出力と、外部から入力された入力データとを用いて所定の規則で演算して入力データを暗号化して最終的な暗号化データとして出力するようにされ、最終的な暗号化データが暗号化されるデータにフィードバックされると共に、暗号化データを得るための演算に用いる暗号化の出力がリセット信号によりリセットされるため、同一データの連続入力を利用したデータ窃取が行えないと共に、暗号化データの伝送系によるデータエラーなどに対する復元力を有する。

この発明によれば、暗号化回路にＣＦＢモードを取り入れ、ビデオデータの暗号化の際に、出力された暗号化データを暗号器の入力にフィードバックしているため、従来技術で第７図を用いて説明したようなデータ窃取方法で暗号化画像データを窃取して元の画像データを復元しようとしても、元の画像データを全く復元することができないと

いう効果がある。これは、ＣＦＢモードの特徴として、暗号器で発生される疑似乱数列が入力データ列に影響されるため、従来技術で説明した窃取方法により得られた疑似乱数列と、暗号化回路において暗号器で発生される疑似乱数列とが全く異なるからである。

また、この発明によれば、暗号化データを暗号器の入力にフィードバックさせる際に、フィードバックする暗号化データをホールドし、ホールドされた暗号化データをライン毎にリセットしているため、前ラインでの暗号化データによるフィードバックの影響が全くなくなり、前ラインで同期外れや画素欠落などの事故が生じた場合でも、ラインが更新された際に完全に復帰できるという効果がある。

図面の簡単な説明

第１図は、ディジタルデータの暗号化を行う一例の構成を概略的に示すブロック図、第２図は、ＥＣＢモードによる暗号化回路の一例の構成を示すブロック図、第３図Ａおよび第３図Ｂは、ＣＢＣモードによる暗号化回路の一例の構成を示すブロック図、第４図Ａおよび第４図Ｂは、ＣＦＢモードによる暗号化回路の一例の構成を示すブロック図、第５図Ａおよび第５図Ｂは、ＯＦＢモードによる暗号化回路の一例の構成を示すブロック図、第６図Ａおよび第６図Ｂは、カウンタモードによる暗号化回路の一例の構成を示すブロック図、第７図は、映像データ窃取を実現するための一例のシステムを概略的に示すブロック図、第８図は、この発明の実施の一形態に適用可能な映像投影システムの一例の構成を概略的に示すブロック図、第９図は、ＨＤ－ＳＤＩ暗号化装置の一例の構成を示すブロック図、第１０図は、この発明の実施の一形態による暗号化回路の一例の構成を示すブロック図、第１１図は、この発明の実施の一形態による暗号化回路に対応する復号

化回路の一例の構成を示すブロック図である。

発明を実施するための最良の形態

以下、この発明の実施の一形態を、図面を参照しながら説明する。第８図は、この発明の実施の一形態に適用可能な映像投影システムの一例の構成を概略的に示す。この映像投影システムは、ディジタルデータとして提供された映像データを映画館などで上映する際に用いて好適なものである。ビデオデコーダ１０は、例えば図示されない映像サーバからネットワークなどを介して供給された、圧縮符号化された映像データをデコードし、ベースバンドのビデオデータとする。このビデオデータは、例えばＨＤ－ＳＤＩのフォーマットに乗せられ、伝送レートが略１．５Ｇｂｐｓのシリアルディジタルデータとして出力される。

なお、ビデオデコーダ１０は、例えば大容量の光ディスクといった記録媒体に圧縮符号化されて記録された映像データをビデオデコーダ１０で再生し、デコードして出力するようにしてもよい。

ビデオデコーダ１０から出力されたデータは、同軸ケーブル１１を介してＨＤ－ＳＤＩ暗号化装置１２に供給される。ＨＤ－ＳＤＩ暗号化装置１２は、供給されたデータから映像データを抽出して暗号化を施し、暗号化ビデオデータとし、この暗号化ビデオデータを再びＨＤ－ＳＤＩのフォーマットに乗せて出力する。暗号化の際の鍵（Ｋ）は、例えば、ＲＳ２３２Ｃなどのインターフェイスを介して接続されたコンピュータ装置（ＰＣ）から供給される。ＨＤ－ＳＤＩ暗号化装置１２から出力されたデータは、同軸ケーブル１３を介してプロジェクタ１６側に伝送され、ＨＤ－ＳＤＩ復号化装置１４に供給される。

ＨＤ－ＳＤＩ復号化装置１４は、ＨＤ－ＳＤＩフォーマットのディ

ジタルデータから暗号化ビデオデータを抽出して暗号を復号化し、元のベースバンドのビデオデータに戻す。復号化の際の鍵（Ｋ）は、ＨＤ－ＳＤＩ暗号化装置１２において暗号化の際に用いられた鍵（Ｋ）と共通の鍵が用いられ、例えば、ＲＳ－２３２Ｃなどのインターフェイスを介して接続されたコンピュータ装置から供給される。

ＨＤ－ＳＤＩ復号化装置１４で復元されたベースバンドのビデオデータは、同軸ケーブル１５を介してプロジェクタ１６に供給され、プロジェクタ１６により図示されないスクリーンに投影される。

なお、上述では、ビデオデコーダ１０とＨＤ－ＳＤＩ暗号化装置１２とが別個の装置であるように説明したが、実際には、ＨＤ－ＳＤＩ暗号化装置１２は、ビデオデコーダ１０に組み込まれて用いられる。この場合には、ビデオデコーダ１０とＨＤ－ＳＤＩ暗号化装置１２とを接続する同軸ケーブル１１を省略することができ、また、ビデオデコーダ１０から出力されるビデオデータをＨＤ－ＳＤＩのフォーマットに乗せずに、例えばパラレルのディジタルデータとして扱うことができる。ＨＤ－ＳＤＩ復号装置１４も同様にして、プロジェクタ１６に組み込まれて用いられる。この場合にも同様に、同時期ケーブル１５を省略することができると共に、ＨＤ－ＳＤＩ復号装置１４からパラレルディジタルデータとしてビデオデータを出力することができる。

第９図は、ＨＤ－ＳＤＩ暗号化装置１２の一例の構成を示す。ＨＤ－ＳＤＩ暗号化装置１２は、概略的には、ＨＤ－ＳＤＩシリアル／パラレル変換回路ブロック２０、暗号回路ブロック３０およびＨＤ－ＳＤＩパラレル／シリアル変換回路ブロック４０から構成される。

ＨＤ－ＳＤＩフォーマットに乗せられ、同軸ケーブル１１を介して伝送されたディジタルデータは、ＨＤ－ＳＤＩシリアル／パラレル変

換回路ブロック２０に供給されてパラレルのディジタルデータに変換され、ビデオデータ、オーディオデータおよびメタデータが取り出される。オーディオデータおよびメタデータは、ＨＤ－ＳＤＩパラレル／シリアル変換回路ブロック４０に供給され、ビデオデータは、暗号化回路ブロック３０で暗号化されてＨＤ－ＳＤＩパラレル／シリアル変換回路ブロック４０に供給される。ＨＤ－ＳＤＩパラレル／シリアル変換回路ブロック４０では、オーディオデータおよびメタデータと、暗号化された暗号化ビデオデータとを重畳し、ＨＤ－ＳＤＩフォーマットに準じたシリアルディジタルデータに変換して出力する。

ＨＤ－ＳＤＩシリアル／パラレル変換回路ブロック２０において、入力されたＨＤ－ＳＤＩフォーマットのシリアルディジタルデータは、ケーブルイコライザ（ＥＱ）／クロック復元回路２１で、伝送時に同軸ケーブル１１により劣化した周波数特性が補正されると共に、クロックが抽出される。ディジタルデータは、受信時に信号が反転しても受信可能なように、ＮＲＺＩ符号化されて信号の方向性が除去されている。ケーブルイコライザ／クロック復元回路２１から出力されたディジタルデータは、ＮＲＺＩ回路２２に供給され、送信時に施されたＮＲＺＩ符号が復号化される。ＮＲＺＩ回路２２の出力は、デスクランブラ２３でデータの送信時にＤＣ成分を除去するために施されたスクランブル処理が解除され、シンク検出回路２４でワード同期が検出され、検出されたワード同期に基づきシリアル／パラレル変換回路２５でパラレルのディジタルデータに変換される。

シリアル／パラレル変換回路２５の出力は、デマルチプレクサ２６に供給され、多重化されているビデオデータ、オーディオデータおよびメタデータなどが分離される。デマルチプレクサ２６で分離されたオーディオデータおよびメタデータは、ＨＤ－ＳＤＩパラレル／シリ

アル変換回路ブロック４０のマルチプレクサ／フォーマッタ４１に供給される。

一方、デマルチプレクサ２６で分離されたビデオデータは、暗号回路ブロック３０に供給され、暗号化回路３１で暗号化される。暗号回路ブロック３０は、ＣＰＵ(Central Processing Unit)３２を有し、例えばＲＳ－２３２Ｃといった所定のインターフェイスを介して外部のコンピュータ装置と通信を行うことができる。暗号回路ブロック３０そのものをコンピュータ装置で構成し、例えば所定の記録媒体に記録されて提供される暗号化プログラムに従い、暗号化処理を行わせてもよい。暗号化回路３１において暗号化の際に用いられる鍵（Ｋ）は、外部のコンピュータ装置から所定のインターフェイスを介して供給され、ＣＰＵ３２を介して暗号化回路３１に与えられる。暗号化回路３１で暗号化された暗号化ビデオデータは、ＨＤ－ＳＤＩパラレル／シリアル変換回路ブロック４０のマルチプレクサ／フォーマッタ４１に供給される。

ＨＤ－ＳＤＩパラレル／シリアル変換回路ブロック４０において、マルチプレクサ／フォーマッタ４１は、供給されたオーディオデータ、メタデータおよび暗号化ビデオデータを多重化し、ＨＤ－ＳＤＩフォーマットにマッピングする。マルチプレクサ／フォーマッタ４１の出力は、パラレル／シリアル変換回路４２でシリアルディジタルデータに変換され、スクランブラ４３でスクランブル処理されＤＣ成分を除去され、ＮＲＺＩ回路４４で上述したＮＲＺＩ符号化される。ＮＲＺＩ回路４４の出力は、ケーブルドライバ４５で伝送レベルまで増幅され、同軸ケーブル１３に対して送り出される。

なお、ＨＤ－ＳＤＩ復号化装置１４は、このＨＤ－ＳＤＩ暗号化装置１２におけるＨＤ－ＳＤＩシリアル／パラレル変換回路ブロック２

０と同様の回路（ＨＤ－ＳＤＩシリアル／パラレル変換回路ブロック２０’とする）と、暗号回路ブロック３０に対応する復号回路ブロックとを有する。復号回路ブロックをコンピュータで構成し、所定の記録媒体に記録された復号プログラムに従い、復号化処理を行わせてもよい。同軸ケーブル１３を介して供給されたＨＤ－ＳＤＩフォーマットのディジタルデータは、ＨＤ－ＳＤＩシリアル／パラレル変換回路ブロック２０’において上述のＨＤ－ＳＤＩシリアル／パラレル変換回路ブロック２０と同様の処理がなされ、暗号化ビデオデータ、オーディオデータおよびメタデータが取り出される。暗号化ビデオデータは、復号回路ブロックに供給され外部のコンピュータ装置から供給された鍵（Ｋ）を用いて復号化され、ベースバンドのビデオデータが復元される。復元されたデータのうち、ビデオデータおよびメタデータは、プロジェクタ１６に供給される。また、オーディオデータは、図示されないオーディオシステムに供給される。

第１０図は、この発明の実施の一形態による暗号化回路３１の一例の構成を示す。この発明の実施の一形態による暗号化回路３１は、カウンタモードによるデータエラーからの復元性と、ＣＦＢモードによる、データ窃取に対する堅牢性とを兼ね備えた構成を実現している。

暗号器１０５は、１２８ビットの長さの鍵（Ｋ）を用いてＡＥＳによる暗号化を施すＡＥＳ暗号器である。なお、暗号器１０５において利用可能な暗号化方式は、ＡＥＳに限られない。ＤＥＳなどのデータをブロック化して暗号化する方式であれば、他の暗号化方式を用いることもできる。また、鍵（Ｋ）のデータ長も１２８ビットに限定されない。

ＣＰＵ＋タイミングコントローラ１１０は、第９図に示したＣＰＵ３２と、図示されないタイミングコントローラからなる。タイミング

コントローラは、クロックと共に、ビデオデータのフレームおよびラインに対応したタイミングで各種信号を出力することができる。

暗号化回路３１に対して、１画素分のデータが輝度Ｙおよび色差Ｃそれぞれ１０ビットずつを割り当てたデータ幅が２０ビットからなるビデオデータが、クロック毎に１画素ずつ入力される。このビデオデータは、ＥＸＯＲ回路１００に供給され、後述するＰ／Ｐシフトレジスタ１０６の出力との排他論理和をとられ、暗号化ビデオデータとされて出力される。

ＥＸＯＲ回路１００から出力された暗号化ビデオデータは、外部すなわちＨＤ－ＳＤＩパラレル／シリアル変換回路ブロック４０に対して出力される。それと共に、暗号化ビデオデータは、フリップフロップ（ＦＦ）回路１０１に供給され、ホールドされる。ＦＦ回路１０１は、ＡＥＳ暗号器１０５と同一のクロック１０７によりホールド値が更新される。また、ＦＦ回路１０１は、ビデオデータのラインが更新される毎に所定の回数リセットするように、ＣＰＵ＋タイミングコントローラ１１０からリセット信号１１９が供給される。リセット信号１１９の回数は、例えば、ＡＥＳ暗号器１０５へのリセット値がＡＥＳ暗号器１０５の出力に反映される、ＡＥＳレーテンシ分に対応した回数とされる。

なお、この実施の一形態では、ＦＦ回路１０１に対して、データ幅が２０ビットの暗号化ビデオデータのうち一部、例えば１６ビットだけが入力される。用いられる１６ビットは、元の暗号化ビデオデータの２０ビットのデータ幅のうちＬＳＢ側、ＭＳＢ側のうち何れでもよいし、２０ビットの中から所定の１６ビットを用いてもよい。なお、これはこの例に限らず、ＦＦ回路１０１に対して暗号化ビデオデータの２０ビット全てを入力することもできるし、１６ビットより少ない

ビット数で入力するようにしてもよい。

ラインカウンタ１０２は、ＣＰＵ＋タイミングコントローラ１１０からビデオデータのライン毎に供給されるトリガ信号１１８によりカウント値を更新するカウンタである。例えば、ラインカウンタ１０２は、ビデオデータのライン毎に、カウント値を１だけカウントアップする。また、ラインカウンタ１０２は、フレームが更新される毎に１回リセットされるように、ＣＰＵ＋タイミングコントローラ１１０からリセット信号１１７が供給される。ラインカウント値は、例えば１６ビットのデータである。

なお、ラインカウンタ１０２は、この例に限られず、複数ライン毎にカウント値を更新するようにしてもよい。また、カウント値の更新も、１ずつカウントするのに限られず、２以上の所定値毎にカウントアップしてもよいし、所定値からカウントダウンするようにしてもよい。さらに、リセット信号１１７によるリセットの際にカウント値が０になるようにリセットしてもよいし、０以外の所定値になるようにリセットすることもできる。さらにまた、ラインカウント値のデータ長は１６ビットに限られない。

フレームカウンタ１０３は、ＣＰＵ＋タイミングコントローラ１１０からビデオデータのフレーム毎に供給されるトリガ信号１１６によりカウント値を更新するカウンタである。例えば、フレームカウンタ１０３は、ビデオデータのフレーム毎に、カウント値を１だけカウントアップする。フレームカウンタ１０３は、例えばビデオデータのプログラムの開始時に１回リセットするように、ＣＰＵ＋タイミングコントローラ１１０からリセット信号１１４が供給される。フレームカウント値は、例えば２４ビットのデータである。

なお、フレームカウンタ１０３は、この例に限られず、カウント値

の更新を、１ずつカウントするのに限られず、２以上の所定値毎にカウントアップしてもよいし、所定値からカウントダウンするようにしてもよい。また、リセット信号１１７によるリセットの際にカウント値が０になるようにリセットしてもよいし、０以外の所定値になるようにリセットすることもできる。さらに、リセット信号１１４も、プログラムの先頭でリセットするのに限らず、例えば所定数のフレーム数毎にリセットするようなものでもよい。さらにまた、ラインカウント値のデータ長は１６ビットに限られない。

ＦＦ回路１０４は、ＣＰＵ＋タイミングコントローラ１１０から与えられるデータ１１２をホールドする。このデータ１１２は、上述したフレームやラインのデータとは異なるデータであって、例えばバージョン情報といった固定値を用いてもよいし、所定の規則、例えばトリガ信号１１３に基づく所定のタイミングで更新される値であってもよい。ＦＦ回路１０４の出力は、例えば７２ビットのデータである。ＦＦ回路１０４の出力は、リセット信号１１１により所定のタイミングでリセットすることができる。なお、ＦＦ回路１０４の出力のデータ長は、７２ビットに限定されない。

上述のＦＦ回路１０４、フレームカウンタ１０３、ラインカウンタ１０２およびＦＦ回路１０１にそれぞれホールドされたデータは、ＡＥＳ暗号器１０５のクロックタイミングで並列的にＡＥＳ暗号器１０５に読み出される。すなわち、この第１０図の例では、ＦＦ回路１０４にホールドされた７２ビットのデータと、フレームカウンタ１０３にホールドされた２４ビットのデータと、ラインカウンタ１０２にホールドされた１６ビットのデータと、ＦＦ回路１０１にホールドされた１６ビットのデータとからなる１２８ビットのデータが、ＡＥＳ暗号器１０５のクロックタイミングで、ＡＥＳ暗号器１０５に入力され

る。

一方、ＣＰＵ＋タイミングコントローラ１１０からＡＥＳ暗号器１０５に対して、鍵長が１２８ビットの鍵（Ｋ）が与えられる。ＡＥＳ暗号器１０５は、上述のＦＦ回路１０４、フレームカウンタ１０３、ラインカウンタ１０２およびＦＦ回路１０１から入力された１２８ビットのデータに対して、鍵（Ｋ）を用いて暗号化を施す。暗号化されて得られた１２８ビットの暗号化データは、そのうちの所定の１２０ビットだけがＰ／Ｐシフトレジスタ１０６に供給される。

Ｐ／Ｐシフトレジスタ１０６は、供給された１２０ビットの暗号化データを、入力されるビデオデータのデータ幅に合わせて２０ビットずつに分割する。したがって、ＡＥＳ暗号器１０５を動作させるためのクロックは、画像データに同期したクロックの１／６の周波数となっている。Ｐ／Ｐシフトレジスタ１０６から出力された２０ビットのデータがＥＸＯＲ回路１００に供給される。ＥＸＯＲ回路１００では、上述したように、入力されたビデオデータとＰ／Ｐシフトレジスタ１０６からの出力との排他論理和をとることで、入力されたビデオデータを暗号化して出力する。

このように、この発明による暗号化回路３１では、暗号化された暗号化データをＡＥＳ暗号器１０５の入力にフィードバックしているため、従来技術で第７図を用いて説明したようなデータ窃取方法で暗号化画像データを窃取して元の画像データを復元しようとしても、元の画像データを全く復元することができない。これは、ＣＦＢモードの特徴として、暗号器で発生される疑似乱数列が入力データ列に影響されるため、従来技術で説明した窃取方法により得られた疑似乱数列と、暗号化回路３１においてＡＥＳ暗号器１０５で発生される疑似乱数列とが全く異なるからである。

また、暗号化データをＡＥＳ暗号器１０５の入力にフィードバックさせる際に、フィードバックする暗号化データをホールドするＦＦ回路１０４に対してライン毎のリセットを行っているため、前ラインでの暗号化データによるフィードバックの影響が全くなくなる。したがって、前ラインで同期外れや画素欠落などの事故が生じた場合、ＣＦＢモードでは当該ライン上にある暗号データの復号は不可能であるが、本発明の方式によれば、ラインが更新された際に完全に復帰できることを意味する。

なお、上述では、ＡＥＳ暗号器１０５に入力されるデータをＦＦ回路１０４、フレームカウンタ１０３、ラインカウンタ１０２およびＦＦ回路１０１の出力としたが、これはこの例に限定されない。例えば、ＦＦ回路１０４による固定値出力を省略することができる。また、フレームカウンタ１０３およびラインカウンタ１０２に対して更新およびリセット周期が異なるカウンタをさらに追加してもよいし、フレームカウンタ１０３を省略することも可能である。さらに、上述では、ＦＦ回路１０４、フレームカウンタ１０３、ラインカウンタ１０２およびＦＦ回路１０１の出力データのビット配分を、ＦＦ回路１０４が７２ビット、フレームカウンタ１０３が２４ビット、ラインカウンタ１０２およびＦＦ回路１０１がそれぞれ１６ビットとしたが、これはこの例に限定されず、他のビット配分でもよい。さらにまた、入力されるビデオデータのビット幅も、２０ビットに限定されず、ビデオ信号の形式も輝度Ｙ、色差Ｃによるものに限定されない。

ここで、特許請求の範囲との一例の対応関係を示すと、請求項１において、保持手段は、例えばＦＦ回路１０１に対応する。１または複数のカウンタは、例えばフレームカウンタ１０３およびラインカウンタ１０２に対応する。暗号化手段は、例えばＡＥＳ暗号器１０５に対

応する。演算手段は、例えばＥＸＯＲ回路１００に対応する。演算手段から出力された暗号化データの一部または全部を保持手段に入力する経路は、例えばＥＸＯＲ回路１００の出力がＦＦ回路１０１に供給される経路に対応する。信号発生手段は、例えばＣＰＵ＋タイミングコントローラ１１０に対応する。なお、これらの対応関係は一例であって、これに限定されるものではない。

第１１図は、第１０図に示す暗号化回路３１に対応する復号化回路１５０の一例の構成を示す。この復号化回路１５０は、ＨＤ－ＳＤＩ復号装置１４に組み込まれて用いられ、ＨＤ－ＳＤＩ暗号化装置１２から同軸ケーブル１３を介して伝送された暗号化ビデオデータを復号化する。復号化回路１５０は、暗号化回路３１におけるＦＦ回路１０１に対して入力される暗号化ビデオデータの入力経路が異なる以外、同一の構成で実現できる。また、復号化回路１５０において、各種のタイミングやデータのビット幅などは、上述の暗号化回路３１と対応させられる。

復号化回路１５０において、ＡＥＳ暗号器１２５は、上述した暗号化回路３１で用いられるＡＥＳ暗号器１０５と同一の回路であって、入力されたデータに対して、暗号化回路３１と共通の鍵である１２８ビットの長さの鍵（Ｋ）を用いてＡＥＳによる暗号化を施す。また、ＣＰＵ＋タイミングコントローラ１３０は、ＣＰＵとタイミングコントローラからなる。タイミングコントローラは、クロックと共に、ビデオデータのフレームおよびラインに対応したタイミングで各種信号を出力することができる。

復号化回路１５０に対して、１画素分に対応する暗号化ビデオデータがデータ幅２０ビットで以てクロック毎に入力される。この暗号化ビデオデータは、ＥＸＯＲ回路１２０に供給され、後述するＰ／Ｐシ

フトレジスタ１２６の出力との排他論理和をとられ、暗号化ビデオデータが復号化され元のデータが復元された復元ビデオデータとされて出力される。

暗号化ビデオデータは、ＥＸＯＲ回路１２０に供給されると共に、２０ビットのうち上述のＦＦ回路１０１で用いられたのに対応する１６ビットがＦＦ回路１２１に供給され、ホールドされる。勿論、上述のＦＦ回路１０１において入力ビデオデータの２０ビットの全てが用いられた場合、ＦＦ回路１２１には、暗号化ビデオデータの２０ビット全てが入力される。ＦＦ回路１２１は、ＡＥＳ暗号器１２５と同一のクロック１４０によりホールド値が更新される。また、ＦＦ回路１２１は、ビデオデータのラインが更新される毎に所定の回数リセットするように、ＣＰＵ＋タイミングコントローラ１３０からリセット信号１３９が供給される。リセット信号１３９のタイミングは、例えば、ＡＥＳ暗号器１２５へのリセット値がＡＥＳ暗号器１２５の出力に反映される、ＡＥＳレーテンシ分とされる。

ラインカウンタ１２２は、上述のラインカウンタ１０２に対応して更新されるカウンタであり、ＣＰＵ＋タイミングコントローラ１３０から暗号化ビデオデータのライン毎に供給されるトリガ信号１３８により、例えば暗号化ビデオデータのライン毎にカウント値を１だけカウントアップしてカウント値を更新する。また、ラインカウンタ１２２は、フレームが更新される毎に１回リセットされるように、ＣＰＵ＋タイミングコントローラ１３０からリセット信号１３７が供給される。ラインカウント値は、例えば１６ビットのデータである。

フレームカウンタ１２３は、上述のフレームカウンタ１０３に対応して更新されるカウンタであり、ＣＰＵ＋タイミングコントローラ１３０から暗号化ビデオデータのフレーム毎に供給されるトリガ信号１

３６により、例えば暗号化ビデオデータのフレーム毎にカウント値を１だけカウントアップしてカウント値を更新するカウンタである。フレームカウンタ１２３は、例えば暗号化ビデオデータのプログラムの開始時に１回リセットするように、ＣＰＵ＋タイミングコントローラ１３０からリセット信号１３４が供給される。フレームカウント値は、例えば２４ビットのデータである。

ＦＦ回路１２４は、ＣＰＵ＋タイミングコントローラ１３０から与えられるデータ１３２をホールドする。このデータ１３２は、上述したフレームやラインのデータとは異なるデータであって、例えばバージョン情報といった固定値を用いてもよいし、所定の規則、例えばトリガ信号１３３に基づく所定のタイミングで更新される値であってもよい。例えば、このデータ１３２は、上述のデータ１１２に対応する値が用いられる。上述したように、データ１１２としてトリガ信号１１３に基づく所定のタイミングで更新される値を用いたときは、データ１３２は、例えば、トリガ１１３に対応するトリガ信号１３３に基づく所定のタイミングで更新される値ととすることができる。ＦＦ回路１２４の出力は、例えば７２ビットのデータである。ＦＦ回路１２４の出力は、上述のリセット信号１１１に対応するタイミングのリセット信号１３１によりリセットすることができる。

上述のＦＦ回路１２４、フレームカウンタ１２３、ラインカウンタ１２２およびＦＦ回路１２１にそれぞれホールドされたデータは、ＡＥＳ暗号器１２５のクロックタイミングで並列的にＡＥＳ暗号器１２５に読み出される。すなわち、この第１１図の例では、ＦＦ回路１２４にホールドされた７２ビットのデータと、フレームカウンタ１２３にホールドされた２４ビットのデータと、ラインカウンタ１２２にホールドされた１６ビットのデータと、ＦＦ回路１２１にホールドされ

た１６ビットのデータとからなる１２８ビットのデータが、ＡＥＳ暗号器１２５のクロックタイミングで、ＡＥＳ暗号器１２５に入力される。

一方、ＣＰＵ＋タイミングコントローラ１３０からＡＥＳ暗号器１２５に対して、鍵長が１２８ビットの鍵（Ｋ）が与えられる。この鍵（Ｋ）は、上述した暗号化回路３１で用いられる鍵（Ｋ）と共通する鍵である。ＡＥＳ暗号器１２５は、上述のＦＦ回路１２４、フレームカウンタ１２３、ラインカウンタ１２２およびＦＦ回路１２１から入力された１２８ビットのデータに対して、鍵（Ｋ）を用いて暗号化を施す。暗号化されて得られた１２８ビットの暗号化データは、そのうちの所定の１２０ビットだけがＰ／Ｐシフトレジスタ１２６に供給される。

Ｐ／Ｐシフトレジスタ１２６は、供給された１２０ビットの暗号化データを、入力される暗号化ビデオデータのデータ幅に合わせて２０ビットずつに分割する。したがって、ＡＥＳ暗号器１２５を動作させるためのクロックは、画像データに同期したクロックの１／６の周波数となっている。Ｐ／Ｐシフトレジスタ１２６から出力された２０ビットのデータがＥＸＯＲ回路１２０に供給される。ＥＸＯＲ回路１２０では、上述したように、入力された暗号化ビデオデータとＰ／Ｐシフトレジスタ１２６からの出力との排他論理和をとることで、入力された暗号化ビデオデータを復号化して出力する。

上述したように、この復号化回路１５０は、上述の暗号化回路３１に対応するものである。したがって、ＡＥＳ暗号器１２５にデータを入力するＦＦ回路１２４、フレームカウンタ１２３、ラインカウンタ１２２およびＦＦ回路１２１の構成や動作は、上述の暗号化回路３１におけるＦＦ回路１０４、フレームカウンタ１０３、ラインカウンタ

１０２およびＦＦ回路１０１に対応する。

ここで、特許請求の範囲との一例の対応関係を示すと、請求項１０において、保持手段は、例えばＦＦ回路１２１に対応する。１または複数のカウンタは、例えばフレームカウンタ１２３およびラインカウンタ１２２に対応する。暗号化手段は、例えばＡＥＳ暗号器１２５に対応する。演算手段は、例えばＥＸＯＲ回路１２０に対応する。外部から入力された暗号化データの一部または全部を保持手段に入力する経路は、例えば暗号化ビデオデータがＥＸＯＲ回路１２０に入力されると共にＦＦ回路１２１に供給される経路に対応する。信号発生手段は、例えばＣＰＵ＋タイミングコントローラ１３０に対応する。なお、これらの対応関係は一例であって、これに限定されるものではない。

なお、ここでは、入力されたビデオデータに対してＰ／Ｐシフトレジスタ１０６の出力を作用させ、暗号化ビデオデータを得るためにＥＸＯＲ回路１００を用いているが、これはこの例に限定されない。

また、上述では、ビデオデータ、暗号化ビデオデータの伝送をＨＤ－ＳＤＩの規格に基づき行うように説明したが、これはこの例に限定されるものではなく、この発明は、他の伝送方式に対しても適用可能である。

請 求 の 範 囲

1．入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記データをリセット信号によりリセットする保持手段と、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする1または複数のカウンタと、

上記保持手段で保持された上記データと上記1または複数のカウンタによる1または複数の上記カウント値とを暗号化する暗号化手段と、

上記暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、

上記演算手段から出力された上記暗号化データの一部または全部を上記保持手段に入力する経路と、

上記保持手段および上記1また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記1また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段と

を有することを特徴とする暗号装置。

2．請求の範囲1に記載の暗号装置において、

上記暗号化手段に対して、さらに固定値が入力され、上記暗号化手段は、該固定値と上記保持手段で保持された上記データと上記1または複数のカウント値とを暗号化するようにしたことを特徴とする暗号装置。

3．請求の範囲1に記載の暗号装置において、

上記保持手段に上記保持された上記データをリセットするリセット信号は、上記１また複数のカウンタのうち少なくとも１の上記カウンタに与えられるリセット信号と同期したタイミングで上記保持手段に与えられることを特徴とする暗号装置。

４．請求の範囲１に記載の暗号装置において、

上記入力データは映像データであって、上記保持手段をリセットするリセット信号は上記映像データに同期していることを特徴とする暗号装置。

５．請求の範囲４に記載の暗号装置において、

上記保持手段をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする暗号装置。

６．請求の範囲１に記載の暗号装置において、

上記入力データは映像データであって、上記１または複数のカウンタのうち少なくとも１をリセットするリセット信号は上記映像データに同期していることを特徴とする暗号装置。

７．請求の範囲６に記載の暗号装置において、

上記１または複数のカウンタのうち少なくとも１をリセットするリセット信号は上記映像データのフレームに同期していることを特徴とする暗号装置。

８．請求の範囲６に記載の暗号装置において、

上記１または複数のカウンタのうち少なくとも１をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする暗号装置。

９．入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記データをリセット信号によりリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化のステップと、

上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップと

を有することを特徴とする暗号方法。

１０．入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記データをリセット信号によりリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化のステップと、

上記暗号化のステップの出力と外部から入力された入力データとを

用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップと

を有する暗号方法をコンピュータ装置に実行させることを特徴とする暗号プログラム。

１１．入力されたデータの一部または全部をトリガ信号により保持し、上記保持された上記データをリセット信号によりリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化のステップと、

上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび

上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップと

を有する暗号方法をコンピュータ装置に実行させる暗号プログラムが記録されたことを特徴とするコンピュータ装置に読み取り可能な記録媒体。

１２．入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持手段と、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウンタと、上記保持手段で保持された上記データと上記１または複数のカウンタによる１または複数の上記カウント値とを暗号化する暗号化手段と、上記暗号化手段の出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、上記演算手段から出力された上記暗号化データの一部または全部を上記保持手段に入力する経路と、上記保持手段および上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段とを有する暗号装置で暗号化された上記暗号化データを復号する復号装置において、

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持手段と、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする

１または複数のカウンタと、

上記保持手段で保持された上記データと上記１または複数のカウンタによる１または複数の上記カウント値とを暗号化する暗号化手段と、

上記暗号化手段の出力と外部から入力された暗号化データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算手段と、

上記外部から入力された上記暗号化データの一部または全部を上記保持手段に入力する経路と、

上記保持手段および上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持手段および上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生手段と

を有することを特徴とする復号装置。

１３．請求の範囲１２に記載の復号装置において、

上記暗号化手段に対して、さらに固定値が入力され、上記暗号化手段は、該固定値と上記保持手段で保持された上記データと上記１または複数のカウント値とを暗号化するようにしたことを特徴とする復号装置。

１４．請求の範囲１２に記載の復号装置において、

上記保持手段に上記保持された上記データをリセットするリセット信号は、上記１また複数のカウンタのうち少なくとも１の上記カウンタに与えられるリセット信号と同期したタイミングで上記保持手段に与えられることを特徴とする復号装置。

１５．請求の範囲１２に記載の復号装置において、

上記暗号化データは映像データが暗号化されたデータであって、上

記保持手段をリセットするリセット信号は上記映像データに同期していることを特徴とする復号装置。

１６．請求の範囲１５に記載の復号装置において、

上記保持手段をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする復号装置。

１７．請求の範囲１２に記載の復号装置において、

上記暗号化データは映像データが暗号化されたデータであって、上記１または複数のカウンタのうち少なくとも１をリセットするリセット信号は上記映像データに同期していることを特徴とする復号装置。

１８．請求の範囲１７に記載の復号装置において、

上記１または複数のカウンタのうち少なくとも１をリセットするリセット信号は上記映像データのフレームに同期していることを特徴とする復号装置。

１９．請求の範囲１７に記載の復号装置において、

上記１または複数のカウンタのうち少なくとも１をリセットするリセット信号は上記映像データのラインに同期していることを特徴とする復号装置。

２０．入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化のステップと、上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入

力データが該暗号化された暗号化データを出力する演算のステップと、上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有する暗号方法で暗号化された上記暗号化データを復号する復号方法において、

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化手段と、

上記暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記外部から入力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップと

を有することを特徴とする復号方法。

２１．入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化のステップと、上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有する暗号方法で暗号化された上記暗号化データを復号する復号方法をコンピュータ装置に実行させる復号プログラムにおいて、

上記復号方法は、

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化手段と、

上記暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記外部から入力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップと

を有することを特徴とする復号プログラム。

２２．入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化のステップと、上記暗号化のステップの出力と外部から入力された入力データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、上記演算のステップから出力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号お

よびリセット信号を、上記保持のステップおよび上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップとを有する暗号方法で暗号化された上記暗号化データを復号する復号方法をコンピュータ装置に実行させる復号プログラムが記録されたコンピュータ装置に読み取り可能な記録媒体において、

上記復号方法は、

入力されたデータの一部または全部をトリガ信号により保持し、リセット信号により上記保持された上記データをリセットする保持のステップと、

トリガ信号によりカウント値をカウントアップまたはカウントダウンし、リセット信号により上記カウント値を所定の値にリセットする１または複数のカウントのステップと、

上記保持のステップで保持された上記データと上記１または複数のカウントのステップによる１または複数の上記カウント値とを暗号化する暗号化手段と、

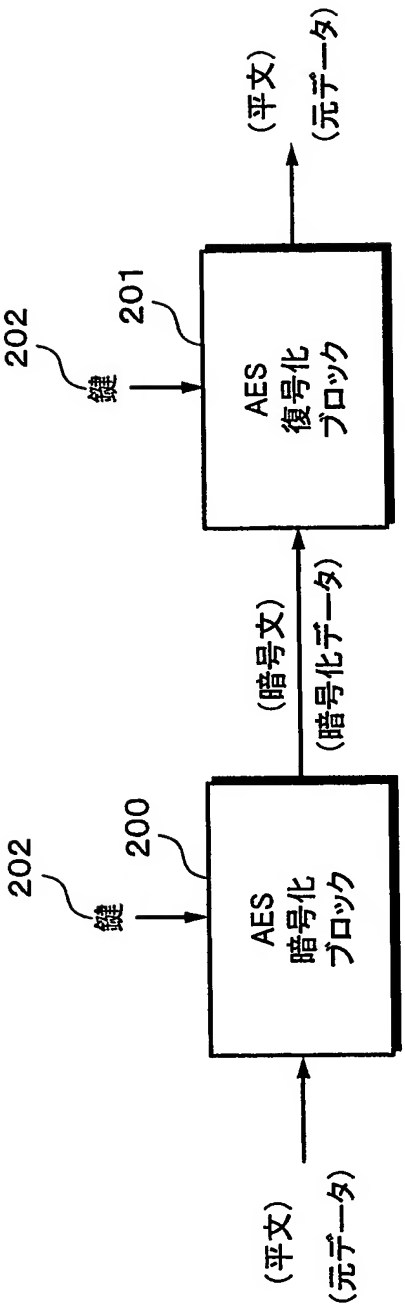
上記暗号化のステップの出力と外部から入力された暗号化データとを用いて所定の規則で演算して上記入力データを暗号化し、該入力データが該暗号化された暗号化データを出力する演算のステップと、

上記外部から入力された上記暗号化データの一部または全部を上記保持のステップに入力するステップと、

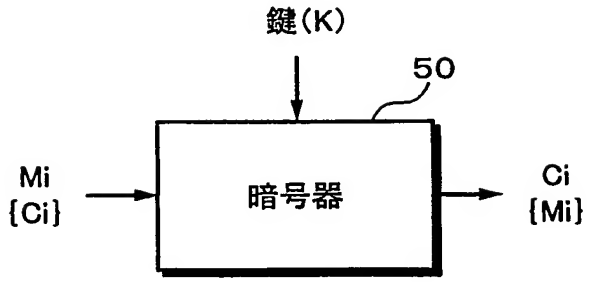
上記保持のステップおよび上記１また複数のカウンタのそれぞれに与えるトリガ信号およびリセット信号を、上記保持のステップおよび上記１また複数のカウンタのそれぞれに所定の規則および／またはタイミングで発生する信号発生のステップと

を有することを特徴とする記録媒体。

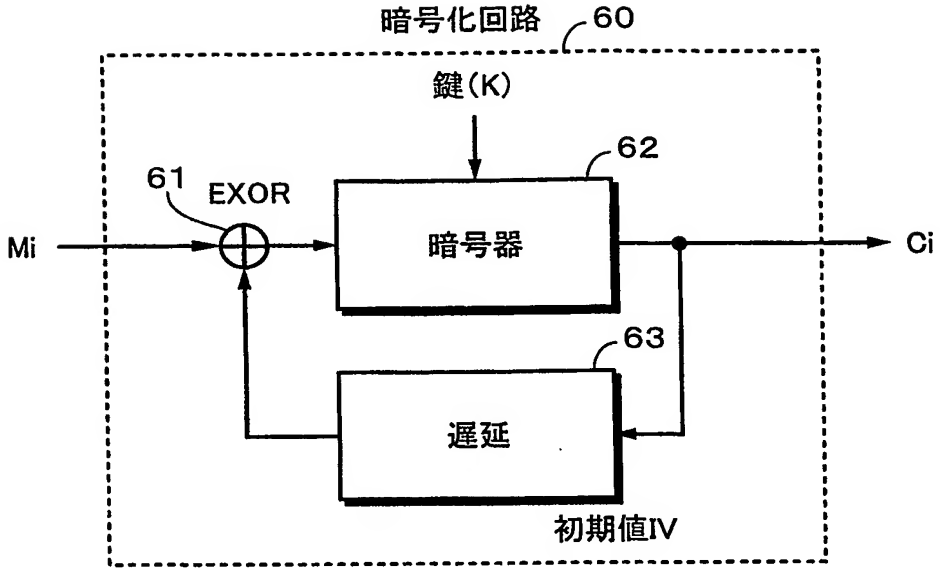
第1図


(平文)
(元データ)
AES
暗号化
ブロック
200
202
鍵
(暗号文)
(暗号化データ)
AES
復号化
ブロック
201
202
鍵
(平文)
(元データ)

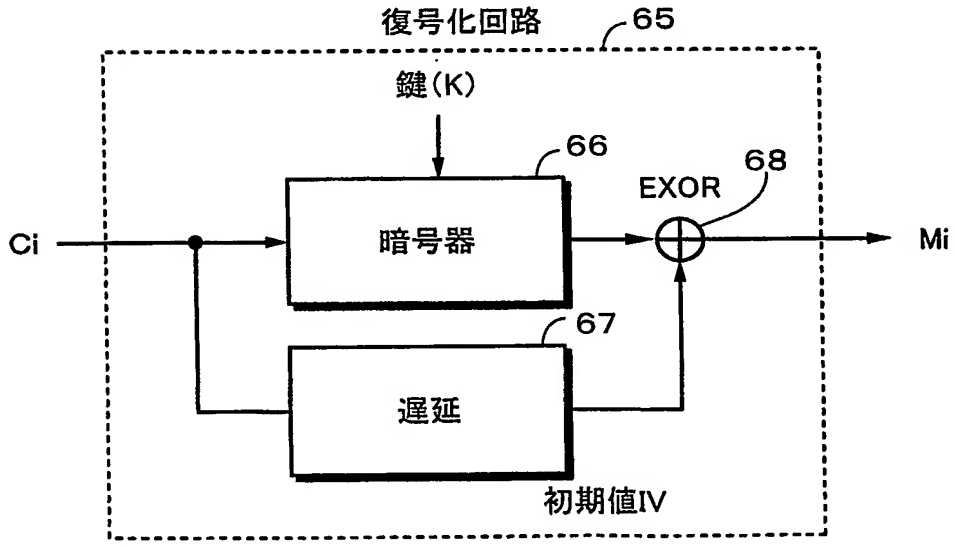
第２図



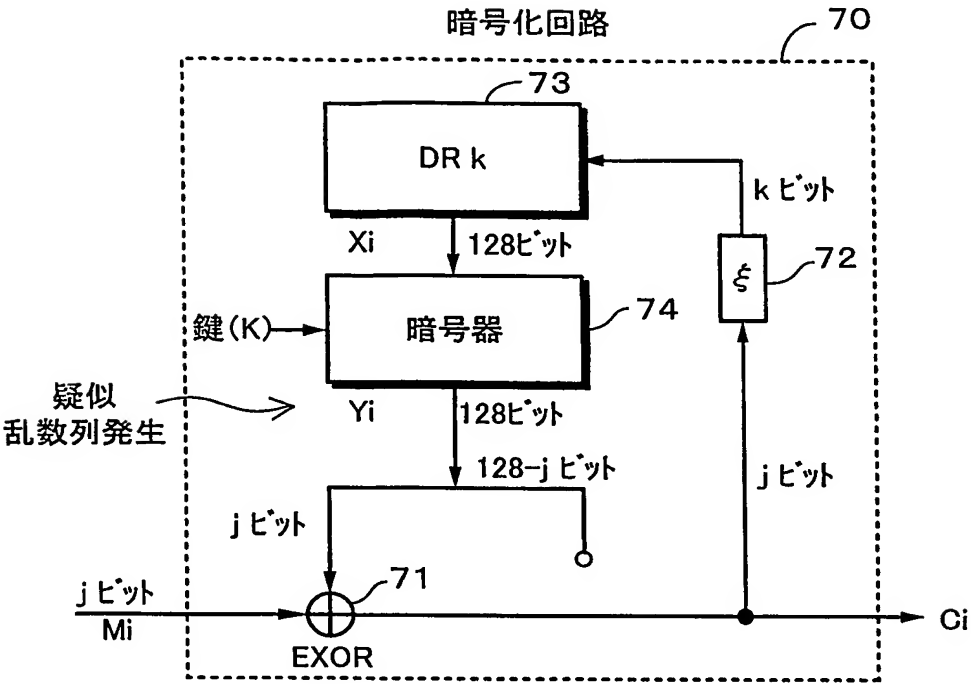
第３図Ａ


暗号化回路
60
鍵(K)
62
61
EXOR
Mi
暗号器
Ci
63
遅延
初期値IV

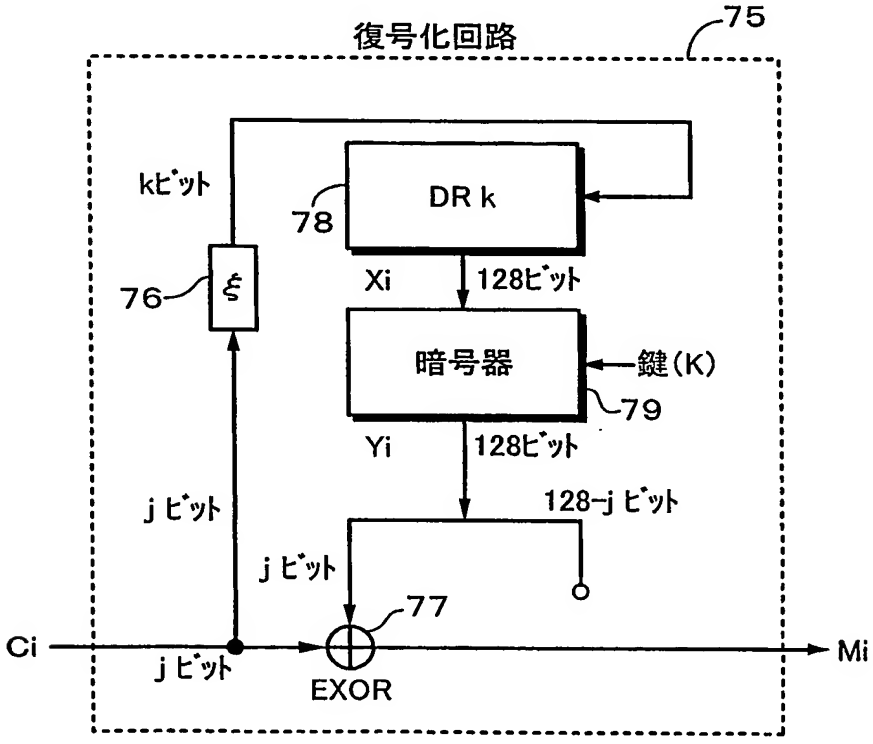
第３図Ｂ


復号化回路
65
鍵(K)
66
68
EXOR
Ci
暗号器
Mi
67
遅延
初期値IV

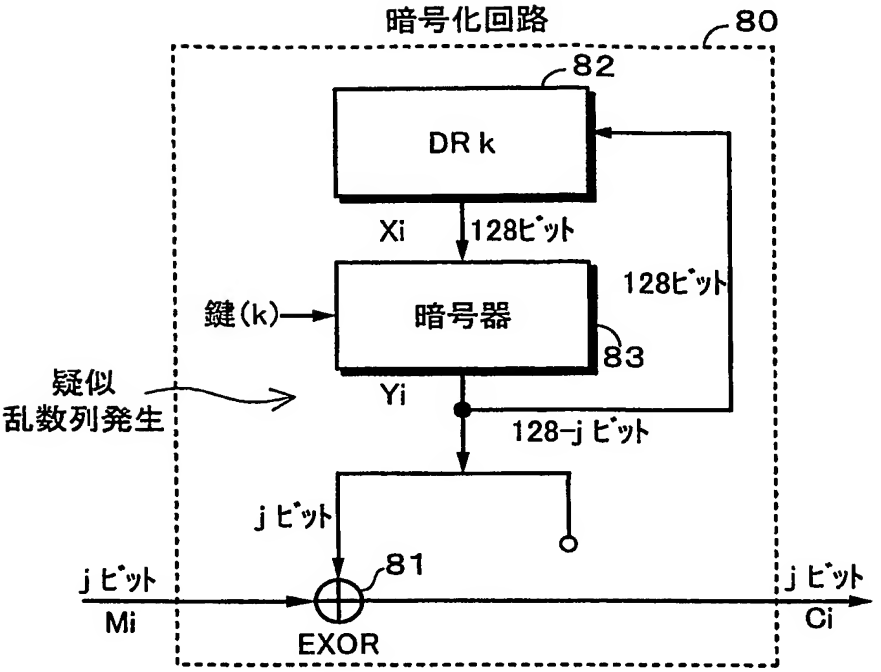
第４図Ａ


暗号化回路
70
73
DR k
k ビット
Xi
128ビット
72
ξ
鍵(K)
暗号器
74
疑似
乱数列発生
Yi
128ビット
128−j ビット
j ビット
j ビット
71
j ビット
Mi
EXOR
Ci

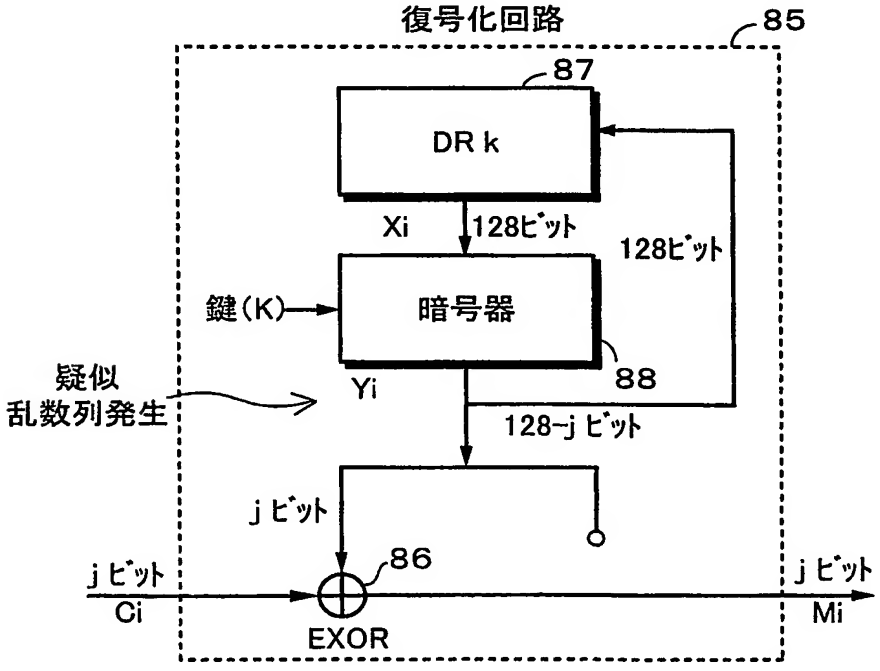
第４図Ｂ


復号化回路
75
kビット
78
DR k
Xi
128ビット
76
ξ
暗号器
鍵(K)
79
Yi
128ビット
128−j ビット
j ビット
j ビット
77
Ci
j ビット
EXOR
Mi

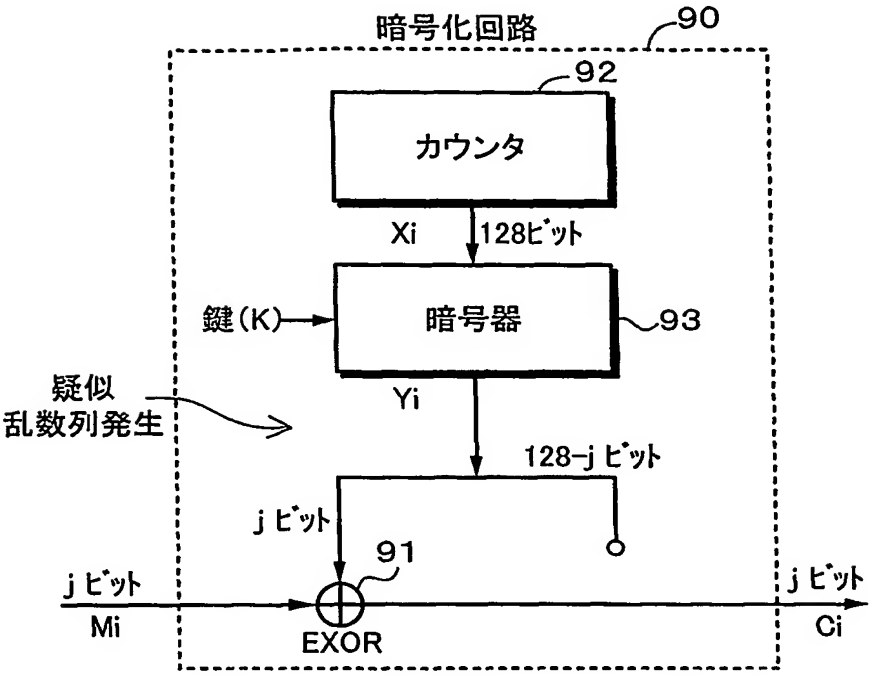
第５図Ａ


暗号化回路
80
82
DR k
Xi
128ビット
128ビット
鍵(k)
暗号器
83
疑似
乱数列発生
Yi
128−j ビット
j ビット
j ビット
Mi
81
EXOR
j ビット
Ci

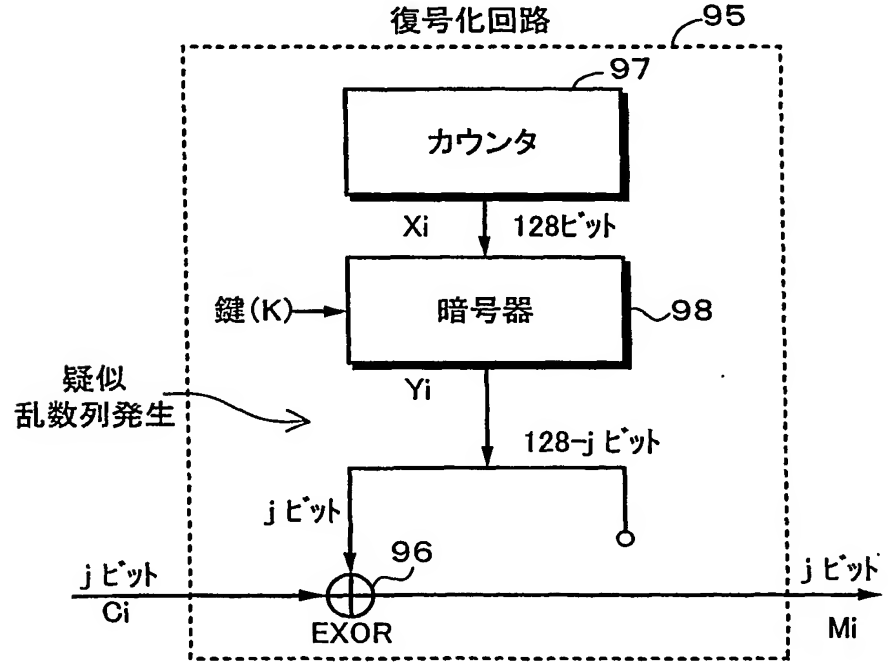
第５図Ｂ


復号化回路
85
87
DR k
Xi
128ビット
128ビット
鍵(K)
暗号器
88
疑似
乱数列発生
Yi
128−j ビット
j ビット
j ビット
Ci
86
EXOR
j ビット
Mi

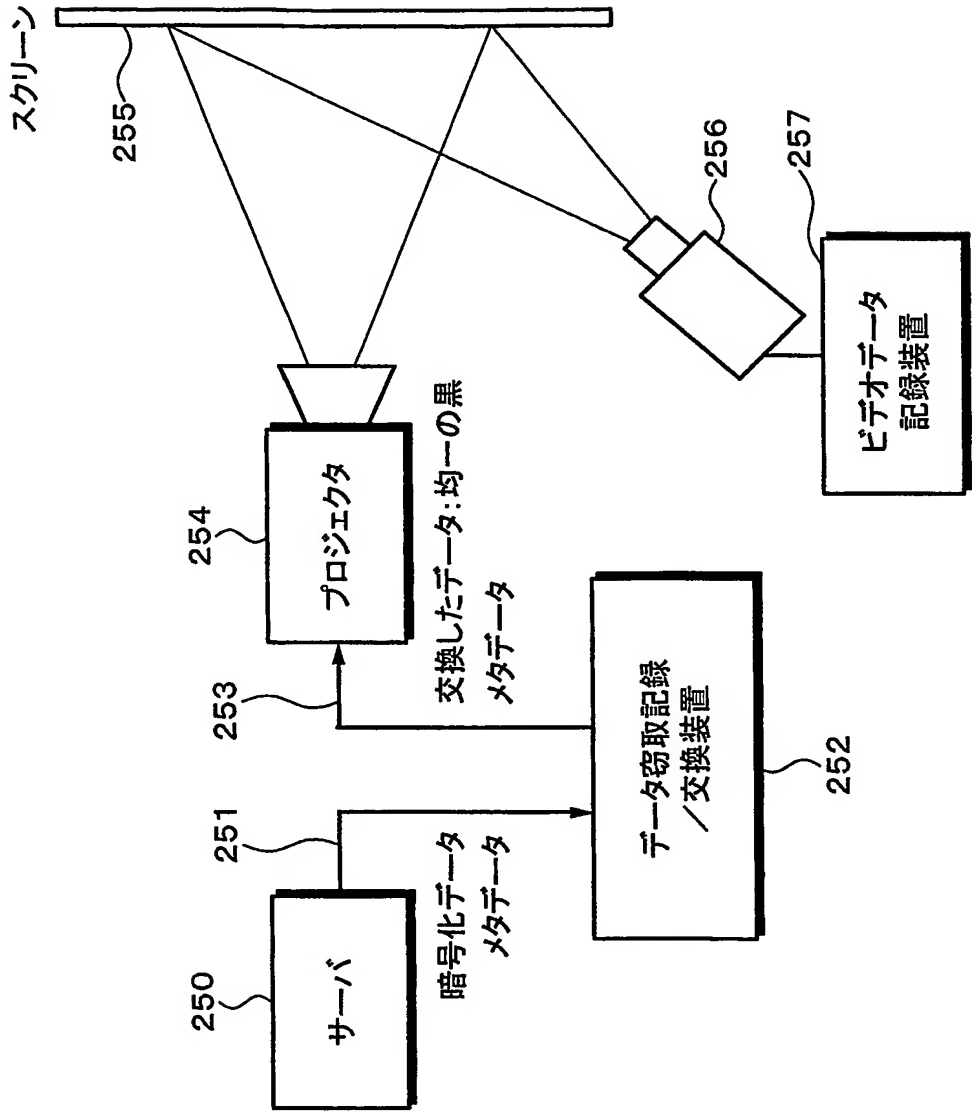
第６図Ａ


暗号化回路
90
92
カウンタ
Xi
128ビット
鍵(K)
暗号器
93
Yi
疑似
乱数列発生
128−j ビット
j ビット
91
j ビット
Mi
EXOR
j ビット
Ci

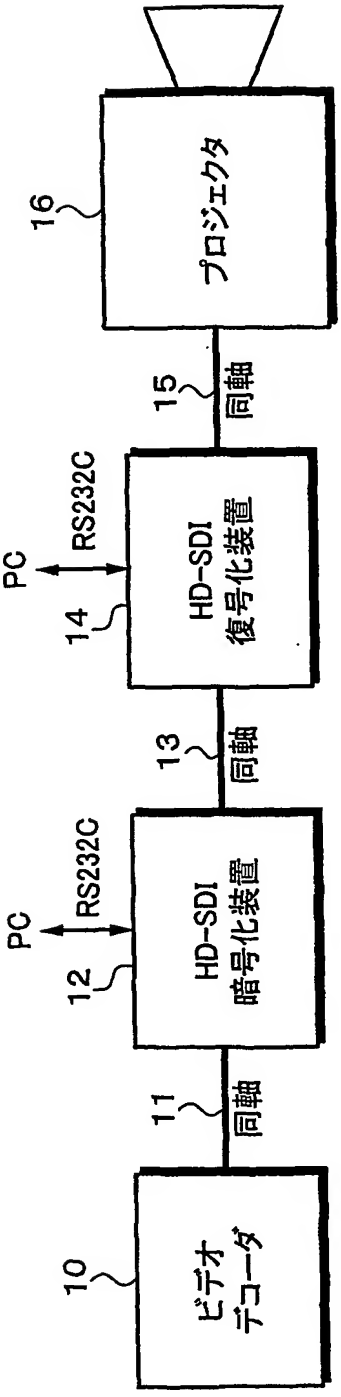
第６図Ｂ


復号化回路
95
97
カウンタ
Xi
128ビット
鍵(K)
暗号器
98
Yi
疑似
乱数列発生
128−j ビット
j ビット
96
j ビット
Ci
EXOR
j ビット
Mi

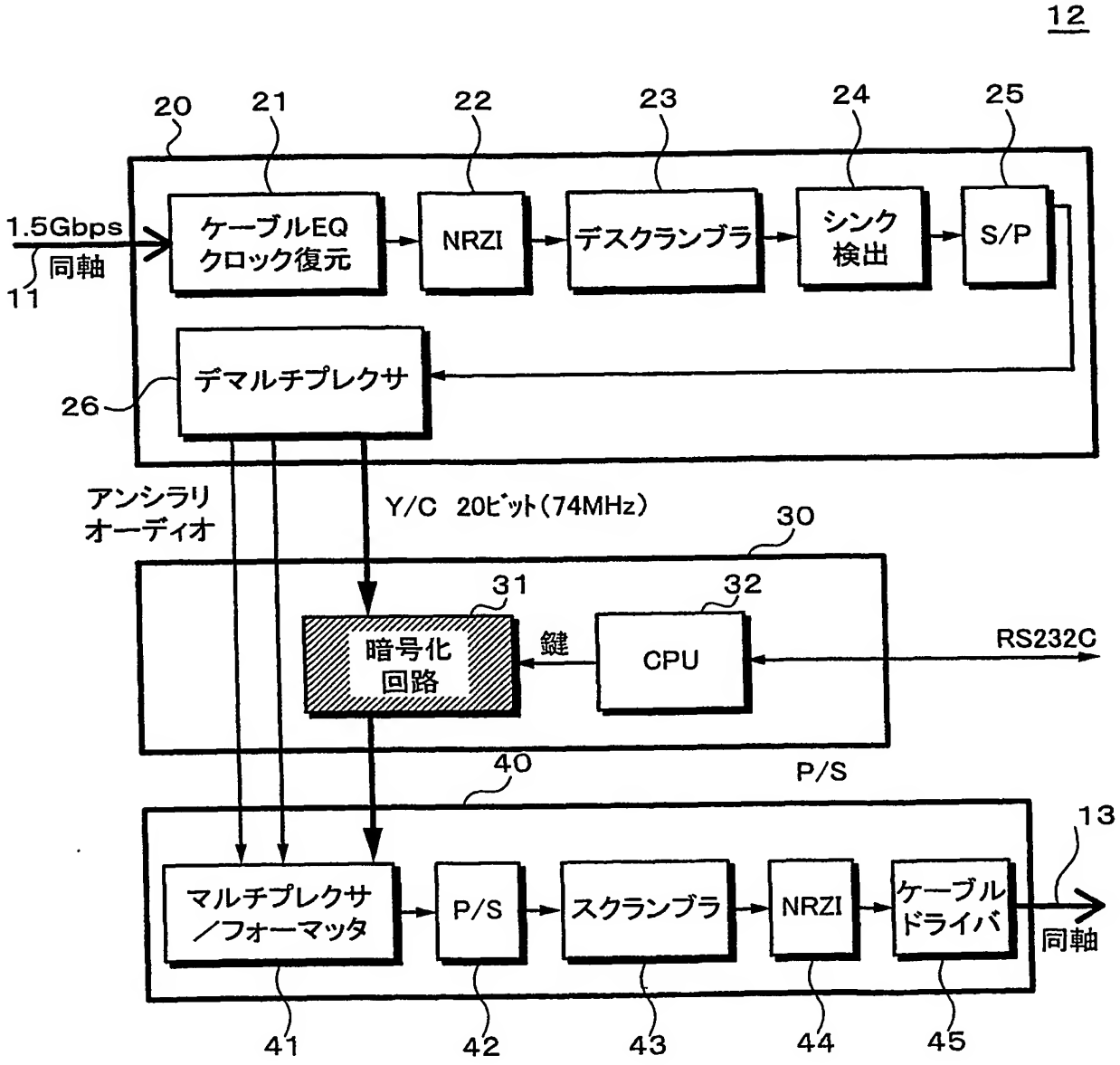
第７図


スクリーン
255
256
257
ビデオデータ
記録装置
プロジェクタ
254
交換したデータ：均一の黒
メタデータ
253
データ窃取記録
／交換装置
252
251
暗号化データ
メタデータ
250
サーバ

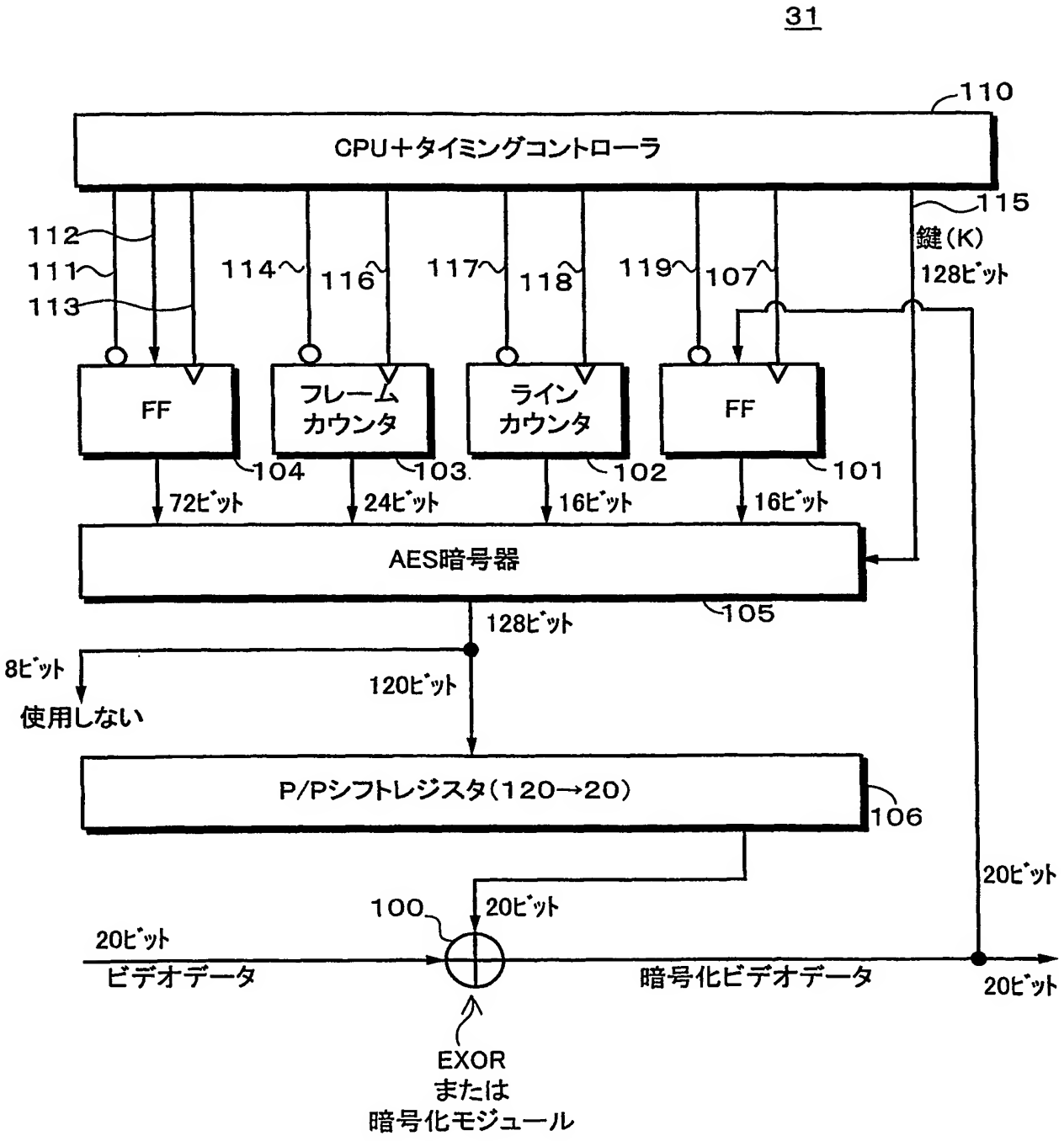
第８図


ビデオ
デコーダ
10
11
同軸
HD-SDI
暗号化装置
12
PC
RS232C
13
同軸
HD-SDI
復号化装置
14
PC
RS232C
15
同軸
プロジェクタ
16

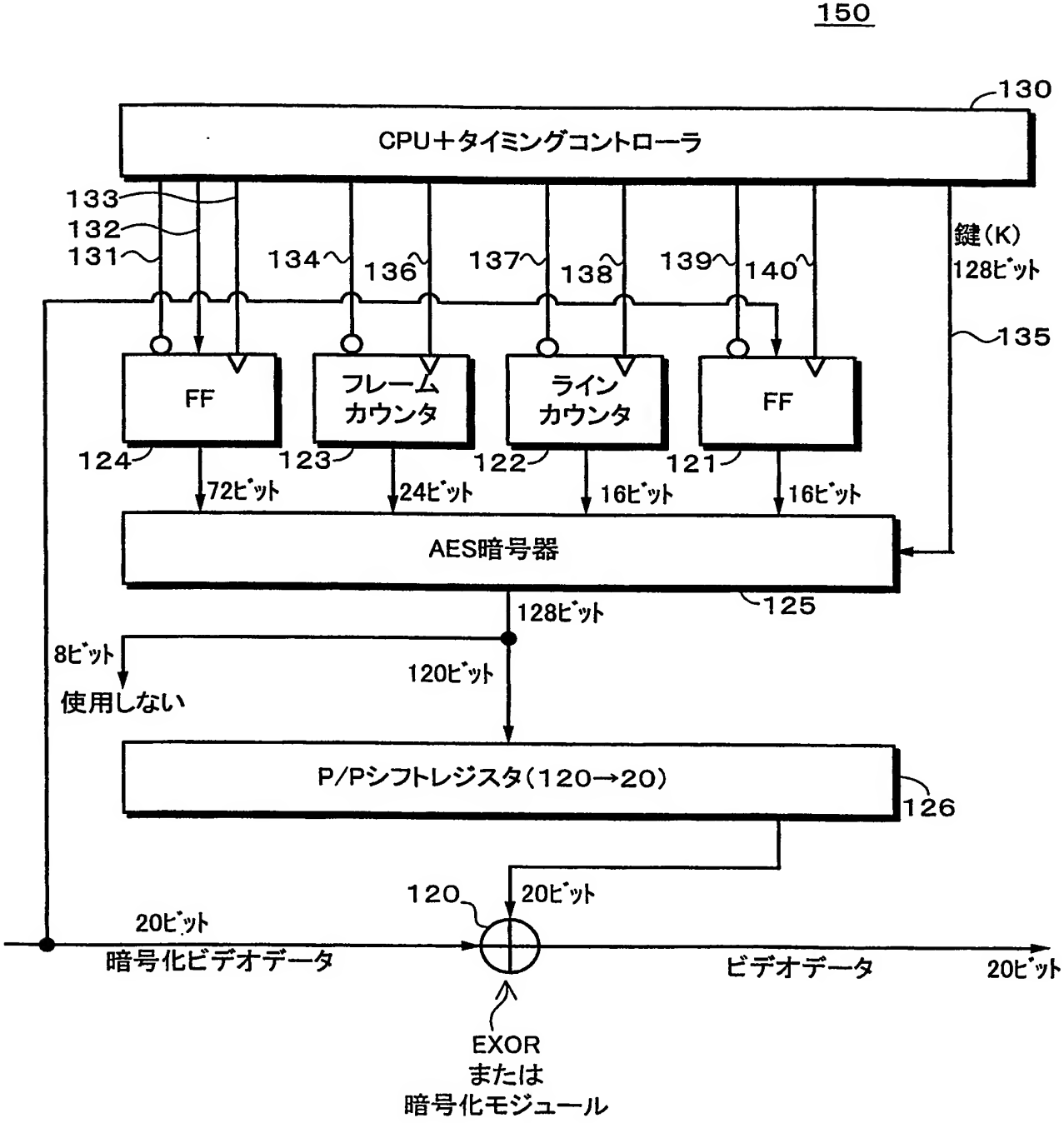
第９図


12
20
21
22
23
24
25
1.5Gbps
同軸
11
ケーブルEQ
クロック復元
NRZI
デスクランブラ
シンク
検出
S/P
デマルチプレクサ
26
アンシラリ
オーディオ
Y/C 20ビット(74MHz)
30
31
32
暗号化
回路
鍵
CPU
RS232C
40
P/S
13
マルチプレクサ
／フォーマッタ
P/S
スクランブラ
NRZI
ケーブル
ドライバ
同軸
41
42
43
44
45

第１０図


31
110
CPU＋タイミングコントローラ
115
鍵(K)
128ビット
112
111
113
114
116
117
118
119
107
FF
フレーム
カウンタ
ライン
カウンタ
FF
104
103
102
101
72ビット
24ビット
16ビット
16ビット
AES暗号器
105
128ビット
8ビット
使用しない
120ビット
P/Pシフトレジスタ(120→20)
106
20ビット
100
20ビット
20ビット
ビデオデータ
暗号化ビデオデータ
20ビット
EXOR
または
暗号化モジュール

第１１図


150
130
CPU＋タイミングコントローラ
133
132
131
134
136
137
138
139
140
鍵(K)
128ﾋﾞｯﾄ
135
FF
フレーム
カウンタ
ライン
カウンタ
FF
124
123
122
121
72ﾋﾞｯﾄ
24ﾋﾞｯﾄ
16ﾋﾞｯﾄ
16ﾋﾞｯﾄ
AES暗号器
125
128ﾋﾞｯﾄ
8ﾋﾞｯﾄ
使用しない
120ﾋﾞｯﾄ
P/Pシフトレジスタ(120→20)
126
120
20ﾋﾞｯﾄ
20ﾋﾞｯﾄ
暗号化ビデオデータ
ビデオデータ
20ﾋﾞｯﾄ
EXOR
または
暗号化モジュール

符　号　の　説　明

１０　ビデオデコーダ

１２　ＨＤ－ＳＤＩ暗号化装置

１３　同軸ケーブル

１４　ＨＤ－ＳＤＩ復号装置

１６　プロジェクタ

２０　ＨＤ－ＳＤＩシリアル／パラレル変換回路ブロック

２６　デマルチプレクサ

３０　暗号回路ブロック

３１　暗号化回路

３２　ＣＰＵ

４０　ＨＤ－ＳＤＩパラレル／シリアル変換回路ブロック

４１　マルチプレクサ／フォーマッタ

５０　復号化回路

１００　ＥＸＯＲ回路

１０１　ＦＦ回路

１０２　ラインカウンタ

１０３　フレームカウンタ

１０４　ＦＦ回路

１０５　ＡＥＳ暗号器

１０６　Ｐ／Ｐシフトレジスタ

１１０　ＣＰＵ＋タイミングコントローラ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009907

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G09C1/00, H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G09C1/00, H04L9/06, H04N7/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Kokai Jitsuyo Shinan Koho 1971-2004
Toroku Jitsuyo Shinan Koho 1994-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), block cipher, counter, feedback

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Jaechul Sung et al., Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation, Lecture Notes in Computer Science, Vol.2288, pages 103 to 113, 2002 especially 3 The CTR-OFB and CTR-CFB Schemes, Appendix: The Figures of the CTR-OFB and CTR-CFB Schemes	1-22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 November, 2004 (12.11.04)	30 November, 2004 (30.11.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　PCT／JP2004／009907

A.　発明の属する分野の分類（国際特許分類（IPC））

Int.Cl⁷ G09C1／00, H04L9/06

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl⁷ G09C1／00, H04L9/06, H04N7／16

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国登録実用新案公報	1994－2004年
日本国公開実用新案公報	1971－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル（JOIS）
block cipher, counter, feedback

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	Jaechul Sung, et.al., Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation, Lecture Notes in Computer Science, Vol.2288, p.103-113, 2002 especially 3 The CTR-OFB and CTR-CFB Schemes, Appendix: The Figures of the CTR-OFB and CTR-CFB Schemes	1-22

☐ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 12. 11. 2004	国際調査報告の発送日 30.11.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正　5M　9364 電話番号　03－3581－1101　内線　3599

様式PCT／ISA／210（第2ページ）（2004年1月）